METHOD AND SYSTEM FOR IDENTITY EXCHANGE AND RECOGNITION FOR GROUPS AND GROUP MEMBERS

Abstract of the Invention

A group certificate is used in a communication system to establish and recognize a group identity at a receiving system. Once a group identity is recognized, members of the group may be recognized based on membership certificates, or they may be recognized based on their own personal certificates separate from the group. In other words a member may be recognized based on trust by the recipient in the group or based on trust by the recipient in the member personally. Group identity information is created for inclusion in the group certificate. A group-signed group certificate is generated, and the certificate has as the group identity information, at least a first key, and a digital signature signed using a second key associated with the first key in the group certificate. The group-signed group certificate is sent to a receiving system to establish the group identity at the receiving system. A group-signed group membership certificate is sent to the receiving system to establish membership of the originator of the membership certificate in the group whose group identity is established at the receiving system. A security protocol is assigned to communications from group members based on the group identity information if the membership certificate is accepted. A security protocol is also assigned to communications from a group member based on a personal identity if a personal certificate is accepted.